Available online at www.sciencedirect.com

ScienceDirect

European Journal of Combinatorics 28 (2007) 674–684

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Notes on Taniguchi's dimensional dual hyperovals

Satoshi Yoshiara

Department of Mathematics, Tokyo Woman's Christian University, Suginami-ku, Tokyo 167-8585, Japan

Received 24 August 2005; accepted 29 January 2006
Available online 28 February 2006

Abstract

The d-dimensional dual hyperoval $\mathcal{T}_\sigma(K)$ constructed by Taniguchi is shown to be a quotient of the d-dimensional dual hyperoval $\mathcal{HV}_d(q)$ constructed by exploiting the Veronesean map. We determine when the d-dimensional dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$ coincides with $\mathcal{T}_{\sigma'}(K)$. Some applications are also included.

1. Introduction

A family $\mathcal{A}$ of d-(projective) dimensional subspaces of a Desarguesian projective space $PG(n,q)$ over a finite field $GF(q)$ is called a (d-dimensional) *dual arc* if the following conditions (i)–(iii) are satisfied:

(i) any two distinct members of $\mathcal{A}$ intersect at a projective point.
(ii) any three mutually distinct members of $\mathcal{A}$ intersect trivially.
(iii) the members of $\mathcal{A}$ generate $PG(n,q)$.

The underlying vector space of dimension $n+1$ over $GF(q)$ for $PG(n,q)$ is called the *ambient space* of $\mathcal{A}$. It is easy to see that $\mathcal{A}$ consists of at most $((q^{d+1}-1)/(q-1))+1$ members. We call $\mathcal{A}$ a d-dimensional *dual hyperoval* over $GF(q)$ if the upper bound is attained.

Let $\mathcal{A}$ and $\overline{\mathcal{A}}$ be d-dimensional dual arcs with ambient spaces U and $\overline{U}$ over $GF(q)$ respectively. We say that $\mathcal{A}$ *covers* $\overline{\mathcal{A}}$ (or $\overline{\mathcal{A}}$ is a *quotient* of $\mathcal{A}$), if $\mathcal{A}$ and $\overline{\mathcal{A}}$ consist of the same number of members and there exists a surjective $GF(q)$-semilinear map ρ from U onto $\overline{U}$ such that every member of $\mathcal{A}$ is mapped isomorphically onto a member of $\overline{\mathcal{A}}$.

For a d-dimensional dual hyperoval, its ambient space has (vector) dimension at least $2d$ and at most $(d+1)(d+2)/2$ (resp. $((d+1)(d+2)/2)+2$ if $q>2$ (resp. $q=2$) by

E-mail address: yoshiara@lab.twcu.ac.jp.

0195-6698/$ - see front matter
doi:10.1016/j.ejc.2006.01.004

[11, Theorem 1]. There are four known constructions of infinite families of d-dimensional dual hyperovals: Veronesean constructions $\mathcal{HV}_d(q)$ in $PG(d(d+3)/2, q)$ for every even power q by Thas and van Maldeghem (see [8] and Section 2.1), characteristic dual hyperovals in $PG(d(d+3)/2, 2)$ by Buratti and Del Fra [1,2] (originally due to Huybrechts [3]), constructions $\mathcal{S}^{d+1}_{\sigma,\phi}$ in $PG(2d+1, 2)$ or $PG(2d, 2)$ exploiting a Galois group generator σ and an o-polynomial ϕ by the author (see [10,9] and Section 3.1), and constructions $\mathcal{T}_\sigma(K)$ by Taniguchi (see [7] and Section 2.2). Comparing with the other constructions, the last one has the following feature: its ambient space may have various dimensions, and the description is simple.

The aim of this note is to investigate relations of $\mathcal{T}_\sigma(K)$ with $\mathcal{HV}_d(q)$ and $\mathcal{S}^{d+1}_{\sigma,\phi}$. In fact, the construction given in [7] may also give a d-dimensional dual arc $\mathcal{T}'_\sigma(K)$ with $(q^{d+1}-1)/(q-1)$ members for every prime power q, not only for even power. Similarly, Veronesean construction gives a d-dimensional dual arc $\mathcal{AV}_d(q)$ with $(q^{d+1}-1)/(q-1)$ members for every prime power q. Thus the author treats those dual arcs of second maximum size as well. To be precise, the following are shown.

(1) (Proposition 1) $\mathcal{T}'_\sigma(K)$ (resp. $\mathcal{T}_\sigma(K)$) is covered by $\mathcal{AV}_d(q)$ (resp. $\mathcal{HV}_d(q)$ if q is even).
(2) (Proposition 3) $\mathcal{T}_\sigma(GF(2^{d+1})) = \mathcal{S}^{d+1}_{\sigma,\phi}$ with $\phi(X) = X^{2^{d+1}-2}$.

These observations yield several nice applications. One is an almost complete solution for the question about dimensions of quotients of $\mathcal{AV}_d(q)$ (Corollary 2), and the other is to calculate the wrapping number for the affine expansion of $\mathcal{HV}_d(q)$ (Corollary 4). The latter is an example which shows the importance of simplicity of the presentation of $\mathcal{T}_\sigma(GF(2^{d+1}))$ given in [7]. Two related problems are also proposed.

2. Veronesean and Taniguchi's constructions

In this section, we use the following notation. Let $q = p^e$ be a power of a prime p with $e \geq 1$, and let d be a positive integer with $d \geq 2$. We denote $I := \{0, 1, \ldots, d\}$ and define subsets $I^{(2)}$ and J of $I \times I$ by

$$I^{(2)} := \{(i, j) \mid i, j \in I, i < j\} \quad \text{and} \quad J := \{(i, i) \mid i \in I\} \cup I^{(2)}.$$

Then $|I| = (d+1)d/2$ and $|J| = (d+1)(d+2)/2$.

For a nonzero vector v of a vector space V, the 1-dimensional subspace of V (projective point of $PG(V)$) spanned by v is denoted $[v]$.

2.1. Veronesean construction

Take vector spaces V and W of dimensions $d+1$ and $(d+1)(d+2)/2$ over $GF(q)$, respectively. We choose a basis $\mathbf{e}_i$ $(i \in I)$ for V indexed by I. Similarly, we take a basis $\mathbf{e}_{(i,j)}$ $((i, j) \in J)$ for W indexed by J. It is convenient to write $\mathbf{e}_{ij} := \mathbf{e}_{(i,j)}$ or $\mathbf{e}_{(j,i)}$ according to whether $(i, j) \in J$ or not. The *Veronesean* map ζ is a map from V to W given by

$$\sum_{i \in I} x_i \mathbf{e}_i \mapsto \sum_{(i,j) \in J} x_i x_j \mathbf{e}_{(i,j)}.$$

The d-dimensional dual arc $\mathcal{AV}_d(q)$ in $PG(W) \cong PG(d(d+3)/2, q)$ is constructed using ζ [11, Subsection 3.1]. It is also given as follows without mentioning ζ [11, Lemma 6, Proposition 7].

For a projective point $P = [\sum_{i\in I} t_i \mathbf{e}_i]$ of $PG(V) \cong PG(d, q)$, we define $A(P)$ to be the subspace of W spanned by

$$\sum_{i\in I} t_i \mathbf{e}_{ij}, \quad \text{where } j \text{ ranges over } I. \tag{1}$$

Notice that for a sequence $(x_j)_{j\in I}$ with $x_j \in GF(q)$ we have

$$\sum_{j\in I} x_j \left(\sum_{i\in I} t_i \mathbf{e}_{ij}\right) = \sum_{i\in I} x_i t_i \mathbf{e}_{(i,i)} + \sum_{(i,j)\in I^{(2)}} (x_i t_j + x_j t_i)\mathbf{e}_{(i,j)}. \tag{2}$$

Using Eq. (2), it is easy to verify that the vectors in Eq. (1) form a basis for $A(P)$ over $GF(q)$. We also define $A(\infty)$ to be the subset of W consisting of vectors

$$\sum_{i\in I} x_i^2 \mathbf{e}_{ii} + 2 \sum_{(i,j)\in I^{(2)}} x_i x_j \mathbf{e}_{(i,j)}, \quad \text{where } x_i \in GF(q) \quad (i \in I). \tag{3}$$

From [11, Proposition 7(1)], the family $\mathcal{AV}_d(q) := \{A(P) \mid P \in PG(V)\}$ is a d-dimensional dual arc in $PG(W)$ with $(q^{d+1} - 1)/(q - 1)$ members. Thus for each $A(P)$ $(P \in PG(V))$ there exists a unique point, say $h(P)$, of $PG(A(P))$ which is not written as $A(P) \cap A(Q)$ for any $Q \in PG(V)$ distinct from P. From [11, Proposition 7(3)], the subset $A(\infty)$ coincides with the set of $h(P)$ $(P \in PG(V))$. If q is even, then $A(\infty)$ is a subspace of W of dimension $d + 1$, whence $\mathcal{HV}_d(q) := \mathcal{AV}_d(q) \cup \{A(\infty)\}$ is a d-dimensional dual hyperoval in $PG(W) \cong PG(d(d + 3)/2, q)$.

2.2. Taniguchi's construction

Let n be an integer with $n \geq d+1$, and regard $GF(q^n)$ and $GF(q^n) \times GF(q^n)$ respectively as n and $2n$-dimensional vector spaces over $GF(q)$. Choose a subspace K of $GF(q^n)$ of dimension $d + 1$ over $GF(q)$ with a basis e_i $(i \in I)$ indexed by I. Take a generator σ of the Galois group $\mathrm{Gal}(GF(q^n)/GF(q))$.

For each projective point P of $PG(K) \cong PG(d, q)$, where $P = [t]$ for $t = \sum_{i\in I} t_i e_i \in K^\times$, consider the following $(d + 1)$-dimensional subspace $T(P)$ of $GF(q^n) \times GF(q^n)$:

$$T(P) := \{(xt, x^\sigma t + xt^\sigma) \mid x \in K\}.$$

We also define a subset $T(\infty)$ of $GF(q^n) \times GF(q^n)$ by

$$T(\infty) := \{(x^2, 2x^{\sigma+1}) \mid x \in K\}.$$

Notice that the arguments in the proof of [7, Theorem 2] excluding the last two paragraphs are valid even when q is odd. Thus $\mathcal{T}'_\sigma(K) := \{T(P) \mid P \in PG(K)\}$ is a d-dimensional dual arc with $(q^{d+1} - 1)/(q - 1)$ members. Then for each $P \in PG(K)$, there exists a unique point $h(P)$ of $PG(T(P))$ which cannot be expressed as $T(P) \cap T(Q)$ for any $Q \in PG(K) \setminus \{P\}$. One can verify that $T(\infty) = \{h(P) \mid P \in PG(K)\}$. If q is even, then $\mathcal{T}_\sigma(K) := \mathcal{T}'_\sigma(K) \cup \{T(\infty)\}$ is a d-dimensional dual hyperoval.

We will describe the ambient space U of $\mathcal{T}'_\sigma(K)$ (or $\mathcal{T}_\sigma(K)$ if q is even). For this purpose, we define a vector $e_{(i,j)}$ of $GF(q^n) \times GF(q^n)$ for $(i, j) \in J$ as follows.

$$e_{(i,i)} := (e_i^2, 2e_i^{\sigma+1}) \quad \text{and} \quad e_{(i,j)} := (e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma) \quad \text{if } i \neq j.$$

It is also convenient to write $e_{ij} := e_{(i,j)}$ or $e_{(j,i)}$ according to whether $(i, j) \in J$ or not.

Elements x and t ($\neq 0$) of K are written as $x = \sum_{i\in I} x_i e_i$ and $t = \sum_{j\in I} t_j e_j$ for some $x_i, t_j \in GF(q)$ $(i, j \in I)$. Then we have

$$\begin{aligned}(xt, x^\sigma t + xt^\sigma) &= \left(\sum_{(i,j)\in I\times I} x_i t_j e_i e_j, \sum_{(i,j)\in I\times I} x_i t_j e_i^\sigma e_j + \sum_{(i,j)\in I\times I} x_i t_j e_i e_j^\sigma\right)\\ &= \sum_{(i,j)\in I\times I} x_i t_j (e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)\\ &= \sum_{i\in I} x_i t_i (e_i^2, 2e_i^{\sigma+1}) + \sum_{(i,j)\in I^{(2)}} (x_i t_j + t_i x_j)(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)\\ &= \sum_{i\in I} x_i t_i e_{(i,i)} + \sum_{(i,j)\in I^{(2)}} (x_i t_j + t_j x_i) e_{(i,j)}\\ &= \sum_{j\in I} x_j \left(\sum_{i\in I} t_i e_{ij}\right).\end{aligned}$$

(The last equation is obtained by the same calculation as Eq. (2).) Hence $T(P)$ for $P = [t]$, $t = \sum_{j\in I} t_j e_j$, is a $(d+1)$-dimensional subspace of $GF(q^n) \times GF(q^n)$ with basis

$$\sum_{i\in I} t_i e_{ij}, \quad \text{where } j \text{ ranges over } I. \tag{4}$$

Similarly, if q is even, then we have $(x^2, 0) = ((\sum_{i\in I} x_i e_i)^2, 0) = \sum_{i\in I} x_i^2 (e_i^2, 0)$. Thus $T(\infty) = \{h(P) \mid P \in PG(K)\}$ is a $(d+1)$-dimensional subspace of $GF(q^n) \times GF(q^n)$ consisting of vectors

$$\sum_{i\in I} x_i^2 e_{(i,i)}, \quad \text{where } x_i \in GF(q) \quad (i \in I). \tag{5}$$

In particular, the ambient space U of $\mathcal{T}'_\sigma(K)$ is the subspace of $GF(q^n) \times GF(q^n)$ spanned by $e_{(i,j)}$ for all pairs $(i, j) \in J$. The subspace U is also the ambient space of a d-dimensional dual hyperoval $\mathcal{T}_\sigma(K)$, if q is even. Notice that the vectors $e_{(i,j)}$ $((i, j) \in J)$ may be linearly dependent over $GF(q)$.

2.3. An observation

We use the notation in Sections 2.1 and 2.2.

Proposition 1. *Let K be any subspace of $GF(q^n)$ of dimension $d+1$ over $GF(q)$ with basis e_i $(i \in I)$. Then Taniguchi's dual arc $\mathcal{T}'_\sigma(K)$ is a quotient of $\mathcal{AV}_d(q)$. If q is even, then Taniguchi's dual hyperoval $\mathcal{T}_\sigma(K)$ is a quotient of $\mathcal{HV}_d(q)$, where $A(\infty)$ corresponds to $T(\infty)$.*

Proof. As we saw in Section 2.1, the ambient space W of $\mathcal{AV}_d(q)$ has a basis $\mathbf{e}_{(i,j)}$ $((i, j) \in J)$. On the other hand, the ambient space U of $\mathcal{T}'_\sigma(K)$ is spanned by $e_{(i,j)}$ $((i, j) \in J)$, as we saw in Section 2.2. We define a $GF(q)$-linear map ρ from W to U by setting

$$(\mathbf{e}_{(i,j)})\rho := e_{(i,j)} \tag{6}$$

on the basis $\mathbf{e}_{(i,j)}$ $((i, j) \in J)$ for W and by extending it onto W by linearity. Then ρ is a $GF(q)$-linear surjection from W onto U.

We will show that ρ sends a member $A(P)$ of $\mathcal{AV}_d(q)$ for a projective point $P = [\sum_{i\in I} t_i \mathbf{e}_i]$ of $PG(V) \cong PG(d,q) \cong PG(K)$ to a member $T(\overline{P})$ of $\mathcal{T}'_\sigma(K)$, where $\overline{P} = [\sum_{i\in I} t_i e_i]$. It follows from Eqs. (1) and (4) that ρ sends a basis $(\sum_{i\in I} t_i \mathbf{e}_{ij})_{j\in I}$ for $A(P)$ to a basis $(\sum_{i\in I} t_i e_{ij})_{j\in I}$ for $T(\overline{P})$. Thus ρ maps $A(P)$ bijectively onto $T(\overline{P})$. Hence ρ gives a quotient map from $\mathcal{AV}_d(q)$ to $\mathcal{T}'_\sigma(K)$.

Assume that q is even. In view of descriptions of $A(\infty)$ and $T(\infty)$ given as (3) and (5), the map ρ sends $A(\infty)$ bijectively onto $T(\infty)$. (This can also be established without comparing the explicit shape of $A(\infty)$ with that of $T(\infty)$, since every d-dimensional dual arc with $(q^{d+1}-1)/(q-1)$ members is uniquely extended to a d-dimensional dual hyperoval [11, Proposition 9].) Thus ρ gives a quotient map from $\mathcal{HV}_d(q)$ to $\mathcal{T}_\sigma(K)$. □

2.4. Quotients of $\mathcal{AV}_d(q)$

We give two remarks which are obtained as corollaries of Proposition 1.

The first one is an alternative proof of [7, Proposition 8]. By [11, Proposition 7(2)], in $\mathcal{AV}_d(q)$, if P, Q, R are three points of $PG(V)$ on a line, then the subspace spanned by $A(P)$ and $A(Q)$ contains $A(R)$. Taking their images by the quotient map ρ from $\mathcal{AV}_d(q)$ to $\mathcal{T}_\sigma(K)$, the corresponding property holds for $\mathcal{T}_\sigma(K)$, which is the property stated in [7, Proposition 8].

The next one is an improvement of [11, Proposition 15], which is almost the best possible.

Corollary 2. *Let q be any prime power. For every integer l with $2d+1 \le l \le d(d+3)/2$, there is a d-dimensional dual arc with $(q^{d+1}-1)/(q-1)$ members (resp. dual hyperoval) in $PG(l,q)$ covered by $\mathcal{AV}_d(q)$ (resp. $\mathcal{HV}_d(q)$ if q is even).*

Proof. Take $K = GF(q^{d+1})$. In the next paragraph, we will verify that the ambient space U of $\mathcal{T}'_\sigma(GF(q^{d+1}))$ coincides with $\tilde{U} := GF(q^{d+1}) \times GF(q^{d+1})$. Then $\mathcal{T}'_\sigma(GF(q^{d+1}))$ (resp. $\mathcal{T}_\sigma(GF(q^{d+1}))$) is a d-dimensional dual arc in $PG(2d+1,q)$ covered by $\mathcal{AV}_d(q)$ (resp. $\mathcal{HV}_d(q)$ if q is even) by Proposition 1. Then the claim follows from [11, Proposition 13].

Thus it suffices to show that $U = \tilde{U}$. This is done in [7, Corollary 6] when q is even. As the proof there depends on the fact that q is even, here we show a proof that is independent of the parity of q. As $T(P) \cap T(Q)$ is a projective point for $P \ne Q \in PG(GF(q^{d+1}))$, the sum $\langle T(P), T(Q)\rangle$ is a hyperplane of $\tilde{U}$. Hence, in order to show that $U = \tilde{U}$, it suffices to verify that U is not a sum of two distinct members of $\mathcal{T}'_\sigma(GF(q^{d+1}))$. Suppose $U = \langle T([\alpha]), T([\beta])\rangle$ for some $\alpha, \beta \in GF(q^{d+1})^\times$ with $[\alpha] \ne [\beta]$. Then for every $\gamma \in GF(q^{d+1})^\times$ and $z \in GF(q^{d+1})$, a vector $(z\gamma, z^\sigma\gamma + z\gamma^\sigma)$ of $T([\gamma])$ is written as $(x\alpha, x^\sigma\alpha + x\alpha^\sigma) + (y\beta, y^\sigma\beta + y\beta^\sigma)$ for some $x, y \in GF(q^{d+1})$. We have $z\gamma = x\alpha + y\beta$ and $z^\sigma\gamma + z\gamma^\sigma = x^\sigma\alpha + x\alpha^\sigma + y^\sigma\beta + y\beta^\sigma$. Substituting the relation $y = (z\gamma - x\alpha)/\beta$ into the last equation, we obtain the following relation after straightforward calculations:

$$(\beta z^\sigma - \beta^\sigma z)\left(\frac{\gamma}{\beta} - \left(\frac{\gamma}{\beta}\right)^\sigma\right) = (\beta\alpha^\sigma - \beta^\sigma\alpha)\left(\frac{x}{\beta} - \left(\frac{x}{\beta}\right)^\sigma\right).$$

This implies that for every $\gamma \in GF(q^{d+1})^\times$ and every $z \in GF(q^{d+1})$, there exists $x \in GF(q^{d+1})$ such that

$$\left(\frac{\beta z^\sigma - \beta^\sigma z}{\beta\alpha^\sigma - \beta^\sigma\alpha}\right) \cdot (\gamma - \gamma^\sigma) = x - x^\sigma. \tag{7}$$

(Remark that the letters γ, z and x are not the same as before.)

Recall that for each $s \in GF(q^{d+1})^\times$, the $GF(q)$-linear map T_s from $GF(q^{d+1})$ to $GF(q)$ defined by $T_s(x) := \mathrm{Tr}_{GF(q^{d+1})/GF(q)}(sx)$ $(x \in GF(q^{d+1}))$ has the following properties, where $\mathrm{Tr}_{GF(q^{d+1})/GF(q)}$ denotes the trace function for the Galois extension $GF(q^{d+1})/GF(q)$ [6, Theorems 2.24, 2.25]: $\mathrm{Ker}(T_s)$ is a hyperplane of $GF(q^{d+1})$, and we have $\mathrm{Ker}(T_s) = \mathrm{Ker}(T_{s'})$ if and only if $[s] = [s']$, where $[s]$ denotes the projective point over $GF(q)$ spanned by s. Moreover, $\mathrm{Ker}(T_1) = \{w - w^\sigma \mid w \in GF(q^{d+1})\}$, because σ generates $\mathrm{Gal}(GF(q^{d+1})/GF(q))$. In terms of $\mathrm{Ker}(T_s)$, the above Eq. (7) is rephrased as follows:

> for every $z \in GF(q^{d+1})$, the kernel $\mathrm{Ker}(T_1)$ is contained in $\mathrm{Ker}(T_s)$, where $s = (\beta z^\sigma - \beta^\sigma z)/(\beta\alpha^\sigma - \beta^\sigma\alpha)$.

Hence $\mathrm{Ker}(T_1) = \mathrm{Ker}(T_s)$, that is, $(\beta z^\sigma - \beta^\sigma z)/(\beta\alpha^\sigma - \beta^\sigma\alpha) \in GF(q)$ for every $z \in GF(q^{d+1})$. Thus the set $I := \{\beta z^\sigma - \beta^\sigma z \mid z \in GF(q^{d+1})\}$ consists of at most q elements. However, I is the image of the $GF(q)$-linear map $GF(q^{d+1}) \ni z \mapsto \beta z^\sigma - \beta^\sigma z \in GF(q^{d+1})$ with kernel $[\beta]$ (notice that for $z \in GF(q^{d+1})^\times$, we have $\beta^{\sigma-1} = z^{\sigma-1}$ iff $z/\beta \in GF(q)^\times$). Thus we have $q^d = |I| \le q$, which contradicts our assumption that $d \ge 2$. □

In Corollary 2, the unique open case is $l = 2d$, namely, we have to determine whether or not $\mathcal{AV}_d(q)$ has a quotient dual arc in $PG(2d, q)$. Related to this question, it is desirable to determine whether $\mathcal{T}'_\sigma(GF(q^{d+1}))$ has a proper quotient or not. By [11, Proposition 13], $\mathcal{T}'_\sigma(GF(q^{d+1}))$ has a proper quotient if and only if there is a projective point $[(\gamma, \delta)]$ of $PG(\tilde{U})$ $(\tilde{U} = GF(q^{d+1}) \times GF(q^{d+1}))$ which is not contained in $\langle T([\alpha]), T([\beta])\rangle$ for any distinct points $[\alpha], [\beta]$ of $PG(GF(q^{d+1}))$. The last condition on (γ, δ) is rephrased as follows: for every $\alpha, \beta \in GF(q^{d+1})^\times$ with $[\alpha] \ne [\beta]$, there is no $x, y \in GF(q^{d+1})$ satisfying

$$(\gamma, \delta) = (x\alpha, x^\sigma\alpha + x\alpha^\sigma) + (y\beta, y^\sigma\beta + y\beta^\sigma). \tag{8}$$

Eliminating $y = (\gamma - \alpha x)/\beta$, we have

$$(x/\beta)^\sigma - (x/\beta) = \frac{\delta - (\beta^{1-\sigma}\gamma^\sigma + \beta^{\sigma-1}\gamma)}{\alpha\beta^\sigma - \alpha^\sigma\beta}.$$

This equation, and hence Eq. (8) has no solutions x, y in $GF(q^{d+1})$ if and only if

$$\mathrm{Tr}_{GF(q^{d+1})/GF(q)}\left(\frac{\delta - (\beta^{1-\sigma}\gamma^\sigma + \beta^{\sigma-1}\gamma)}{\alpha\beta^\sigma - \alpha^\sigma\beta}\right) \ne 0. \tag{9}$$

Although it looks a simple question on arithmetic in finite fields, so far I have not been able to prove or disprove the existence of (γ, δ) $(\ne (0, 0))$ in $\tilde{U}$ satisfying the above condition (9) for all $\alpha, \beta \in GF(q^{d+1})^\times$ with $[\alpha] \ne [\beta]$. The only result I have now is the non-existence of such a pair (γ, δ) for $q = 2$. Thus I propose it as a question.

Problem. Does Taniguchi's dimensional dual arc $\mathcal{T}'_\sigma(GF(q^{d+1}))$ have proper quotient? Namely, does there exist (γ, δ) $(\ne (0, 0))$ in $\tilde{U}$ satisfying condition (9) for all $\alpha, \beta \in GF(q^{d+1})^\times$ with $[\alpha] \ne [\beta]$?

3. Taniguchi's DHO $\mathcal{T}_\sigma(K)$ as $\mathcal{S}^{d+1}_{\sigma,\phi}$

In this section, we investigate relations between dimensional dual hyperovals $\mathcal{T}_\tau(K)$ (Section 2.2) and $\mathcal{S}^{d+1}_{\sigma,\phi}$.

3.1. The dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$

By [10,9], $\mathcal{S}^{d+1}_{\sigma,\phi}$ is a d-dimensional dual hyperoval constructed as follows for a generator σ of $\mathrm{Gal}(GF(q)/GF(2))$ ($q = 2^{d+1}$) and an o-polynomial $\phi(X)$ in $GF(q)[X]$. Recall that a polynomial $\phi(X) \in GF(q)[X]$ is called an o-polynomial if the following three conditions are satisfied:

(i) $\phi(0) = 0$ and $\phi(1) = 1$.
(ii) The map ϕ sending $\alpha \in GF(q)$ to $\phi(\alpha)$ is a bijection from $GF(q)$ to itself.
(iii) For each $s \in GF(q)$, the map ϕ_s is also a bijection from $GF(q)$ to itself, where $\phi_s(\alpha) := (\phi(\alpha + s) + \phi(s))/\alpha$ for $\alpha \in GF(q)^\times$ and $\phi_s(0) = 0$.

We regard $V := GF(q) \times GF(q) = \{(x, y) \mid x, y \in GF(q)\}$ as a $2(d+1)$-dimensional vector space over $GF(2)$. Define a $(d+1)$-dimensional subspace $S(t)$ of V for each $t \in GF(q)$ to be

$$S(t) := \{(x, x^\sigma t + x t^\phi) \mid x \in GF(q)\}.$$

Then $\mathcal{S}^{d+1}_{\sigma,\phi}$ is a d-dimensional dual hyperoval with ambient space V if $\sigma\phi \neq id_{GF(q)}$ [9, Proposition 3].

We are interested in when $\mathcal{S}^{d+1}_{\sigma,\phi}$ is a quotient of $\mathcal{HV}_d(2)$. If $\sigma = \phi$, it is shown that $\mathcal{S}^{d+1}_{\sigma,\sigma}$ is a quotient of the Huybrechts dual hyperoval $\mathcal{H}(\kappa_{d+1})$ [4, Proposition 6.8], which is a d-dimensional dual hyperoval in $PG(d(d+3)/2, 2)$ not isomorphic to $\mathcal{HV}_d(2)$. On the other hand, in the case where $\phi \in \mathrm{Gal}(GF(q)/GF(2))$, the following fact is verified for all $q = 2^{d+1}$ with $d \leq 13$ [5, Result 4.4]:

> if $\sigma \neq \phi$ and $\sigma\phi$ is not the identity map on any nonprime subfield of $GF(q)$, then the affine expansion of $\mathcal{S}^{d+1}_{\sigma,\phi}$ is simply connected.

In view of these results, we conjectured that the above statement holds for every d, if $\phi \in \mathrm{Gal}(GF(q)/GF(2))$ [5, Section 1, Conjecture]. This implies that in this case $\mathcal{S}^{d+1}_{\sigma,\phi}$ is never a proper quotient of any d-dimensional dual hyperoval. Thus it looks like that there is no relation between $\mathcal{S}^{d+1}_{\sigma,\phi}$ and $\mathcal{HV}_d(2)$ when ϕ lies in $\mathrm{Gal}(GF(q)/GF(2))$. What happens if $\phi(X)$ is a general o-polynomial?

3.2. A proposition

In view of Proposition 1, if $\mathcal{S}^{d+1}_{\sigma,\phi}$ coincides with $\mathcal{T}_\tau(K)$ for a $(d+1)$-dimensional subspace K of $GF(2^n)$ ($n \geq d+1$) and a generator τ of $\mathrm{Gal}(GF(2^n)/GF(2))$, it is covered by $\mathcal{HV}_d(2)$. This motivates the following result.

Proposition 3. *Let $q = 2^{d+1}$, σ a generator of $\mathrm{Gal}(GF(q)/GF(2))$, and let $\phi(X)$ be an o-polynomial in $GF(q)[X]$. For an integer n with $n \geq d+1$, let τ be a generator of $\mathrm{Gal}(GF(2^n)/GF(2))$ and let K be a $(d+1)$-dimensional subspace of $GF(2^n)$, regarded as a vector space over $GF(2)$ of dimension n.*

Then the following conditions are equivalent.

(1) *$\mathcal{S}^{d+1}_{\sigma,\phi}$ coincides with $\mathcal{T}_\tau(K)$.*
(2) *$K = GF(q)$ is a subfield of $GF(2^n)$ and the restriction of τ on $GF(q)$ coincides with σ and $\phi(X) = X^{q-2}$.*

Proof. Assume that Condition (1) holds. Then there exists a bijective map ρ from $GF(q)$ to $PG(K) \cup \{\infty\}$ such that $S(t) = T(\rho(t))$ for all $t \in GF(q)$. As K is a vector space over $GF(2)$, we can identify the set $PG(K)$ of projective points of K with $K^\times = K - \{0\}$. As $T(\infty)$ is the unique member of $\mathcal{T}_\tau(K)$ contained in $\{(x, 0) \mid x \in GF(2^n)\}$, we have $\rho(0) = \infty$. Thus

$$S(0) = \{(x, 0) \mid x \in GF(q)\} = \{(y^2, 0) \mid y \in K\} = T(\infty),$$

whence $GF(q) = \{y^2 \mid y \in K\}$. As $x \mapsto x^2$ is a field automorphism of $GF(q)$, this implies that $K = GF(q)$ is a subfield of $GF(2^n)$.

Then ρ is a permutation on $GF(q)^\times = K^\times$. From the definitions of $S(t)$ and $T(\rho(t))$ for $t \in GF(q)^\times$, for each $x \in GF(q)$ there exists $y \in GF(q)$ such that

$$(x, x^\sigma t + xt^\phi) = (y\rho(t), y^\tau \rho(t) + y(\rho(t))^\tau).$$

Hence for every $y \in GF(q)$ and $t \in GF(q)^\times$, setting $s := \rho(t)$, we have

$$y^\sigma (s^\sigma t) + y(st^\phi) = y^\tau s + ys^\tau. \tag{10}$$

Take $s = 1$ and $y = 1$. Then $t + t^\phi = 1 + 1 = 0$ from Eq. (10). As $\phi(X)$ is an o-polynomial and $t \neq 0$, this implies $t = 1$. Then, putting $s = t = 1$ into Eq. (10), we have $y^\tau = y^\sigma$ for all $y \in GF(q)$. Hence the restriction of τ onto $GF(q)$ is σ.

Eq. (10) with $y = s$ implies that $(s^\sigma)^2 t = s^2 t^\phi$, from which

$$s = t^{(\phi-1)/2(\sigma-1)}, \tag{11}$$

where $1/(\sigma - 1)$ and $1/2$ respectively denote the inverse maps of the bijections $x \mapsto x^\sigma/x$ and $x \mapsto x^2$ of $GF(q)^\times$. Using Eq. (11) and the equation $x^\tau = x^\sigma$ $(x \in GF(q))$, the square of the left hand side of Eq. (10) is calculated to be $(y^\sigma)^2 s^2 (s^2)^{\sigma-1} t^2 + y^2 s^2 (t^\phi)^2 = s^2((y^\sigma)^2 t^{\phi+1} + y^2 (t^\phi)^2)$. The square of the right hand side of Eq. (10) is $(y^\sigma)^2 s^2 + y^2 s^2 (s^{(\sigma-1)2}) = s^2((y^\sigma)^2 + y^2 (t^{\phi-1}))$. Hence we have

$$(y^2)^\sigma (1 + t^{\phi+1}) = y^2 (t^{\phi-1} + (t^\phi)^2) \tag{12}$$

for all $y \in GF(q)$ and all $t \in GF(q)^\times$.

If $1 + t^{\phi+1} \neq 0$ for some $t \in GF(q)^\times$, then $(y^2)^{\sigma-1}$ and hence y is uniquely determined by t from Eq. (12), which is a contradiction. Hence $t^{\phi+1} = 1$ for all $t \in GF(q)^\times$, which implies that $\phi(X) = X^{q-2}$.

This completes the claim that Condition (1) implies Condition (2). Conversely, assume that Condition (2) is satisfied. Then we have $S(0) = T(\infty)$. For each $t \in GF(q)^\times$, define $s = \rho(t) = (t^{-1})^{1/(\sigma-1)}$. Then direct calculation shows that

$$y^\sigma (s^\sigma t) + y(st^\phi) = y^\sigma s + ys^\sigma.$$

Thus every element $(ys, y^\sigma s + ys^\sigma)$ of $T([s])$ coincides with an element $(ys, (ys)^\sigma t + (ys)t^\phi)$ of $S(t)$, whence $S(t) = T([s])$ for all $t \in GF(q)^\times$. This proved $\mathcal{S}^{d+1}_{\sigma,\phi} = \mathcal{T}_\tau(K)$. □

3.3. Wrapping number of $Af(\mathcal{HV}_d(2))$

Using Proposition 1 and the fact that $\mathcal{S}^{d+1}_{\sigma,X^{q-2}} = \mathcal{T}_\sigma(GF(q))$ $(q = 2^{d+1})$ established in Proposition 3, we can calculate the wrapping number of the affine expansion $Af(\mathcal{HV}_d(2))$ of the dual hyperoval $\mathcal{HV}_d(2)$. This is an important number to measure the universal cover of $Af(\mathcal{HV}_d(2))$.

We first review a few definitions, stated in a form suitable for our purpose [4, Section 1]. For a d-dimensional dual hyperoval $\mathcal{S}$ with ambient space U over $GF(2)$, its *affine expansion* $Af(\mathcal{S})$ is the incidence system defined on the set of vectors of U (called *points*) and the set of cosets in U/X for all $X \in \mathcal{S}$ (called *blocks*) with incidence determined by inclusion as subsets of U. We can verify that each pair of points (resp. blocks) are incident to either zero or exactly two blocks (resp. points). Thus $Af(\mathcal{S})$ is a *semibiplane*. A pair $L = (\{v_0, v_1\}, \{B_0, B_1\})$ of two points v_i $(i = 0, 1)$ and two blocks B_i $(i = 0, 1)$ is called a *line*, if v_i is incident with B_j for every $i, j \in \{0, 1\}$. In this case, we also write $v_i \in L$ $(i = 0, 1)$.

The *wrapping number* $w(Af(\mathcal{S}))$ is defined as follows. Choose a point v_0 and a line $L = (\{v_0, v_1\}, \{B_0, B_1\})$ through v_0, and denote by $\mathcal{B}(v_0, L)$ the set of blocks through v_0 distinct from B_i $(i = 0, 1)$. We define a permutation $\gamma_{v_0,L}$ on $\mathcal{B}(v_0, L)$ by the following algorithm.

(0) Take $B \in \mathcal{B}(v_0, L)$.
(1) Take a unique point u_0 such that $(\{v_0, u_0\}, \{B_0, B\})$ is a line.
(2) Take a unique block Y such that $(\{u_0, v_1\}, \{B_0, Y\})$ is a line.
(3) Take a unique point u_1 such that $(\{v_1, u_1\}, \{B_1, Y\})$ is a line.
(4) Define $\gamma_{v_0,L}(B)$ to be the unique block for which $(\{u_1, v_0\}, \{B_1, \gamma_{v_0,L}(B)\})$ is a line.

The wrapping number $w(Af(\mathcal{S}))$ is defined to be the maximum order of permutations $\gamma_{v_0,L}$ where (v_0, L) range over all pairs of points and lines with $v_0 \in L$.

By Proposition 1, $\mathcal{T}_\sigma(GF(q))$ is covered by $\mathcal{HV}_d(2)$, where $q = 2^{d+1}$. Then we have $w(Af(\mathcal{HV}_d(2))) = w(\mathcal{T}_\sigma(GF(q)))$ by [4, Proposition 1.2]. This allows us to work with the dimensional dual hyperoval $\mathcal{T}_\sigma(GF(q)) = \mathcal{S}^{d+1}_{\sigma,X^{q-2}}$, which has a simpler presentation than $\mathcal{HV}_d(2)$.

For a while, we will consider the general situation. We set $\mathcal{S} := \mathcal{S}^{d+1}_{\sigma,\phi}$, with $\phi(X)$ a general o-polynomial, and will try to calculate the wrapping number $w(Af(\mathcal{S}))$. To simplify the notation, we set

$$f(x, y) = \frac{x^\phi + y^\phi}{x + y}$$

for distinct $x, y \in GF(q)$.

Since $Af(\mathcal{S})$ admits an automorphism group acting regularly on its points [4, Subsection 3.3], we may assume that $v_0 = (0, 0)$. Then the blocks B_i $(i = 0, 1)$ through $(0, 0)$ in the initial situation of the above algorithm have the following forms for some $a \neq b \in GF(q)$:

$$B_0 = S(a), \quad B_1 = S(b).$$

Now v_1 in the line L is the unique vector distinct from $v_0 = (0, 0)$ contained in $S(a) \cap S(b)$, whence we have

$$v_1 = (f(a, b)^{1/(\sigma-1)}, f(a, b)^{\sigma/(\sigma-1)}a + f(a, b)^{1/(\sigma-1)}a^\phi).$$

The block Y defined in Step (2) in the algorithm above is a coset of some member of $\mathcal{S}$. Thus it has the following form for some $z, s \in GF(q)$: $Y = (0, z) + S(s)$. As $v_1 \in Y$, we have $(0, z) + v_1 \in S(s)$. Thus we obtain

$$z = f(a, b)^{\sigma/(\sigma-1)}(a + s) + f(a, b)^{1/(\sigma-1)}(a^\phi + s^\phi). \tag{13}$$

Take $B = S(t)$ $(t \in GF(q) \setminus \{a, b\})$ in Step (0) of the algorithm. The point u_0 in Step (1) of the algorithm is the unique vector distinct from v_0 contained in $S(a) \cap S(t)$. Thus its expression

is obtained from that of v_1 by replacing b by t:

$$u_0 = (f(a,t)^{1/(\sigma-1)}, f(a,t)^{\sigma/(\sigma-1)}a + f(a,t)^{1/(\sigma-1)}a^{\phi}).$$

As $u_0 \in Y$, we have

$$z = f(a,t)^{\sigma/(\sigma-1)}(a+s) + f(a,t)^{1/(\sigma-1)}(a^{\phi}+s^{\phi}), \tag{14}$$

by replacing b by t in Eq. (13)

As v_0 is contained in $\gamma_{v_0,L}(B)$, we have $\gamma_{v_0,L}(B) = S(u)$ for some $u \in GF(q)$. Note that $u \neq b$, as $S(u) = \gamma_{v_0,L}(B) \neq B_1 = S(b)$. By the algorithm above, we need the expression of u in terms of t, a and b. The expression of u_1 in Step (3) in the algorithm is obtained from that of u_0 by just replacing a and t by b and u, respectively. As $u_1 \in Y$, we also obtain the following Eq. (15) from Eq. (14) by replacing a and t by b and u, respectively.

$$z = f(b,u)^{\sigma/(\sigma-1)}(b+s) + f(b,u)^{1/(\sigma-1)}(b^{\phi}+s^{\phi}). \tag{15}$$

Adding together Eqs. (13) and (14), after some manipulations, we have

$$f(a,s)^{1/(\sigma-1)} = f(a,b)^{1/(\sigma-1)} + f(a,t)^{1/(\sigma-1)}, \tag{16}$$

which implies that s is uniquely determined by a, b and t. Similarly, adding Eqs. (13) and (15), we have

$$f(b,s)^{1/(\sigma-1)} = f(a,b)^{1/(\sigma-1)} + f(b,u)^{1/(\sigma-1)}, \tag{17}$$

which implies that u is uniquely determined by a, b and s. Thus, in principle, u is determined by a, b and t.

Now we restrict to our special situation where $x^{\phi} = x^{-1}$ for $x \in GF(q)^{\times}$ ($q = 2^{d+1}$). Then

$$f(x,y) = \frac{(1/x)+(1/y)}{x+y} = \frac{1}{xy}, \quad f(0,y) = \frac{1}{y^2}$$

for all $x, y \in GF(q)^{\times}$ with $x \neq y$.

We first note that $t = 0$ if and only if $u = 0$. Indeed, suppose $t = 0$ but $u \neq 0$. As $a \neq t = 0$, Eq. (16) reads

$$\left(\frac{1}{as}\right)^{\frac{1}{\sigma-1}} = \left(\frac{1}{ab}\right)^{\frac{1}{\sigma-1}} + \left(\frac{1}{a^2}\right)^{\frac{1}{\sigma-1}}.$$

Multiplying by $a^{1/(\sigma-1)}$, we have $(1/s)^{1/(\sigma-1)} = (1/b)^{1/(\sigma-1)} + (1/a)^{1/(\sigma-1)}$. As $b \neq t = 0$, we have $(1/s)^{1/(\sigma-1)} = (1/a)^{1/(\sigma-1)} + (1/u)^{1/(\sigma-1)}$ from Eq. (17) multiplied by $b^{1/(\sigma-1)}$. However, this implies that $u = b$, which is a contradiction. Thus we have $u = 0$ if $t = 0$. Similarly, one can verify that $u = 0$ yields $t = 0$.

First, we assume that $t \neq 0$, or equivalently $u \neq 0$. Then Eq. (16) reads

$$\left(\frac{1}{as}\right)^{\frac{1}{\sigma-1}} = \left(\frac{1}{ab}\right)^{\frac{1}{\sigma-1}} + \left(\frac{1}{at}\right)^{\frac{1}{\sigma-1}} \quad \text{or} \quad \left(\frac{1}{s}\right)^{\frac{2}{\sigma-1}} = \left(\frac{1}{b}\right)^{\frac{2}{\sigma-1}} + \left(\frac{1}{t}\right)^{\frac{2}{\sigma-1}}$$

according to whether $a \neq 0$ or $a = 0$. In any case we have $(1/s)^{1/(\sigma-1)} = (1/b)^{1/(\sigma-1)} + (1/t)^{1/(\sigma-1)}$. Similarly, from Eq. (17) we have $(1/s)^{1/(\sigma-1)} = (1/b)^{1/(\sigma-1)} + (1/u)^{1/(\sigma-1)}$ or $(1/s)^{1/(\sigma-1)} = (1/a)^{1/(\sigma-1)} + (1/u)^{1/(\sigma-1)}$ according to whether $a = 0$ or $a \neq 0$. Then, in our

setting $\gamma_{v_0,L}(S(t)) = S(u)$, we have $u = t$ if $a = 0$, and

$$(1/u)^{1/(\sigma-1)} = (1/t)^{1/(\sigma-1)} + (1/a)^{1/(\sigma-1)} + (1/b)^{1/(\sigma-1)} \tag{18}$$

if $a \neq 0$.

Returning to the general situation, the above conclusions imply that permutation $\gamma_{v_0,L}$ is the identity if $a = 0$. If $a \neq 0$, set $S(v) := \gamma^2_{v_0,L}(S(t)) = \gamma_{v_0,L}(S(u))$. Then if $t = 0$, we have $u = v = 0$. For $t \neq 0$, we have $u \neq 0$ and $(1/v)^{1/(\sigma-1)} = (1/u)^{1/(\sigma-1)} + (1/a)^{1/(\sigma-1)} + (1/b)^{1/(\sigma-1)}$ by applying Eq. (18) to $S(u)$, whence $v = t$ from Eq. (18). This implies that $\gamma_{v_0,L}$ has order 2 if $a \neq 0$. Hence the maximum order of the permutation $\gamma_{v_0,L}$ is 2. (As $\mathcal{HV}_d(2)$ covers $\mathcal{T}_\sigma(GF(q))$ for any generator σ of $\mathrm{Gal}(GF(q)/GF(2))$, we are allowed to take the squaring map as σ. In this case, $1/(\sigma - 1)$ is the identity, which makes the above calculation a bit easier.) This established the following statement.

Corollary 4. *The wrapping number of the affine expansion of the dimensional dual hyperoval $\mathcal{HV}_d(2)$ is 2.*

The wrapping number of semibiplanes of biaffine D_n-type are known to be smaller than or equal to 2 [4, Lemma 7.1], but so far it is not clear whether any of them have a connection with the affine expansion $Af(\mathcal{HV}_d(2))$. I conclude the note by proposing the following question.

Problem. Give an explicit description of the universal cover of $Af(\mathcal{HV}_d(2))$.

References

[1] M. Buratti, A. Del Fra, Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals, Adv. Geom. 3 (2003) S245–S253 (special volume).
[2] A. Del Fra, S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, Eur. J. Combin. 26 (2005) 173–194.
[3] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AG^*$ geometries, Discrete Math. 255 (2002) 503–532.
[4] A. Pasini, S. Yoshiara, On a new family of flag-transitive semibiplanes, Eur. J. Combin. 22 (2001) 529–545.
[5] A. Pasini, S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, Eur. J. Combin. 22 (2001) 547–560.
[6] R. Lidle, H. Niederreiter, Finite Fields, in: Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachusetts, 1983.
[7] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, Eur. J. Combin. 26 (2005) 95–99.
[8] J. Thas, H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, Q. J. Math. 55 (2004) 99–113.
[9] H. Taniguchi, S. Yoshiara, On dimensional dual hyperovals $\mathcal{S}_{\sigma,\phi}$, Innov. Incidence Geom. 1 (2005) 197–219.
[10] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d + 1, 2)$, Eur. J. Combin. 20 (1999) 589–603.
[11] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Algebra Combin. 19 (2004) 5–23.